



Jak nie dać się okraść w sieci

Kim jest Haker?

haker to osoba, która może włamać się do sieci, komputera lub innych systemów informatycznych

Po co to robi:

```
graph TD; A[Po co to robi:] --> B[dla korzyści finansowych]; A --> C[w celu pozyskania poufnych informacji]; A --> D[chęć udowodnienia własnych umiejętności];
```

dla korzyści finansowych

w celu pozyskania
poufnych informacji

chęć udowodnienia
własnych umiejętności

Rodzaje ataków hakerskich

```
graph TD; A[Rodzaje ataków hakerskich] --> B[Phishing – chodzi o to aby kliknąć]; A --> C[Scam – chodzi o to aby wysłać]; A --> D[Fake shop – chodzi o to aby kupić];
```

Phishing – chodzi o to aby kliknąć

Scam – chodzi o to aby wysłać

Fake shop – chodzi o to aby kupić

Przykład Phishing-u

OVHcloud.pl <5a2fd@ambulances-boularand.fr>
to aj ▾

Szanowny Kliencie!

Jesteśmy zobowiązani poinformować o tym, aby uniknąć zawieszenia nazwy domeny ██████████.pl.

Zadłużenie należy uregulować w wysokości 10.00 euro przed 07/09/2022, pod następującym linkiem:

[Uspokoić się teraz](#)

Dziękujemy za Twoją wierność

Z poważaniem,

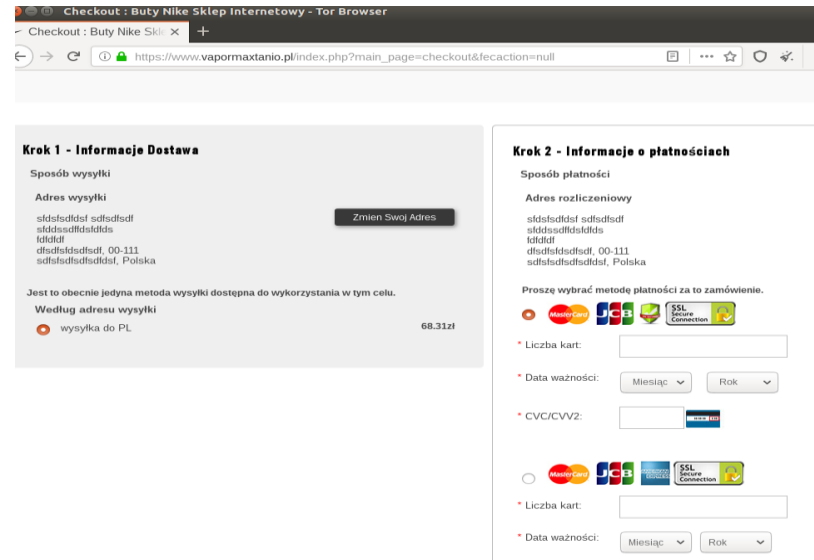
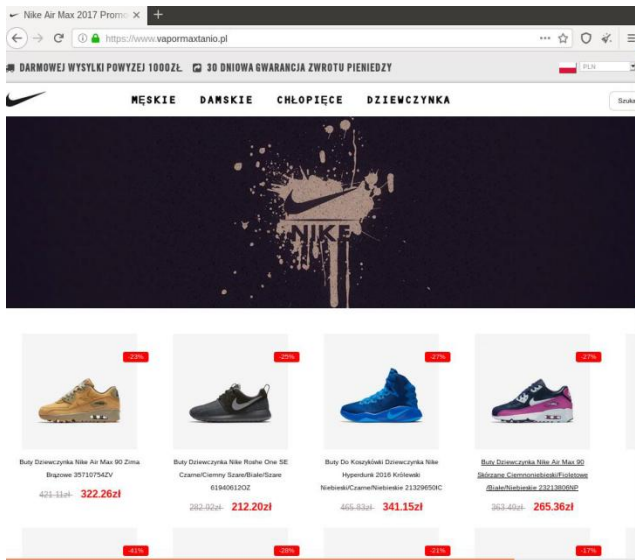
Obsługa klienta OVHcloud

Co zrobić w przypadku otrzymania podobnej wiadomości?

- podejść do sprawy chłodno, dokładnie przeanalizuj wiadomość
- sprawdź adresatów wiadomości
- sprawdź zamieszczone linki
- wprowadź uwierzytelnienia dwuskładnikowe

Przykład Fake Shop-u

Fałszywy sklep



Fałszywe zbiórki na cele charytatywne

Fałszywe giełdy kryptowalut

Co powinno w nas wzbudzić czujność?

- Zaniżone ceny – to nie są okazje
- Duża ilość błędów: literówek, nieprawidłowa odmiana
- Brak opinii lub złe opinie w Google
- Jeden sposób płatności – tylko kartą

Uważaj!

Reklamy w Google nie świadczą o tym, że sklep jest zaufany

Co to jest Scam

- To rodzaj oszustwa internetowego polegający na wykorzystaniu różnych socjotechnik aby wzbudzić współczucie, zaufanie; Głównie chodzi o to aby wyłudzić dane osobowe albo środki pieniężne
- Bardzo często hakerzy podszywają się pod znane marki, np. pocztę lub firmy kurierskie

Co powinno nas zastanowić? Np.

- Nagroda chociaż nie braliśmy udziału w żadnym konkursie
- Niespodziewany spadek otrzymany po zmarłej osobie za granicą
- Prośba o wsparcie dla chorego lub biednej rodziny
- Konieczność opłacenia „paczki”, która jest do nas adresowana
- Znajomy, który kontaktuje się za pomocą komunikatora i potrzebuje naszej pomocy, prosi o podanie kodu BLIK

Co zrobić, gdy daliśmy się „złapać”?

```
graph TD; A[Co zrobić, gdy daliśmy się „złapać”?] --> B[Zmień hasło]; A --> C[Wyloguj się ze wszystkich aktywnych sesji]; A --> D[Sprawdź czy nie „podpięły się” do konta żadne nieznane aplikacje]; A --> E[Zastrzeż kartę/dowód];
```

Zmień hasło

Wyloguj się ze wszystkich aktywnych sesji

Sprawdź czy nie „podpięły się” do konta żadne nieznane aplikacje

Zastrzeż kartę/dowód

Koniecznie zgłos każdą próbę oszustwa. Pomożesz sobie i innym.

← CERT.PL > Zgłos incydent PL EN

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosic osobę kontaktową do CSIRT NASK proszę użyc poniższego odnośnika:

[Zgłoszenie osoby kontaktowej do CSIRT NASK.](#)

Jeżeli chcą Państwo zgłosic złośliwą domenę, proszę użyc poniższego odnośnika:


[Zgłoszenie domeny internetowej służącej do wyludzeń danych i srodkow finansowych.](#)


Zgłoszenie podejrzanych wiadomości SMS


Wszystkie podejrzane wiadomości SMS z linkami można zgłosic używając funkcji "Przekaż", bezpośrednio na numer:


8080

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

 Osoba fizyczna / inne podmioty

 Operator usług kluczowych

 Dostawca usługi cyfrowej

 Podmiot publiczny

Link do zgłoszenia incydentu

<https://incydent.cert.pl/domena#!/lang=pl>

Prezentacja utworzona na podstawie materiałów udostępnionych w ramach **projektu OSEhero** mającego na celu upowszechnianie wiedzy na temat bezpieczeństwa w internecie